strcpy_s() and strcat_s()

Daniel Plakosh, Software Engineering Institute [vita[1]]

Copyright © 2005 Pearson Education, Inc.

2005-09-27; Updated 2008-07-17

L2 / D/P, L[2]

The `strcpy_s()` and `strcat_s()` functions are defined in ISO/IEC TR 24731 as a close replacement for `strcpy()` and `strcat()`. These functions have an additional argument that specifies the maximum size of the destination and also include a return value that indicates whether the operation was successful.

Development Context

Copying and concatenating character strings

Technology Context

C, UNIX, Win32

Attacks

Attacker executes arbitrary code on machine with permissions of compromised process or changes the behavior of the program.

Risk

The `strcpy()` and `strcat()` functions are a source of buffer overflow vulnerabilities.

Description

The `strcpy_s()` and `strcat_s()` functions are defined in ISO/IEC WDTR 24731 as close replacements for `strcpy()` and `strcat()`. These functions take an extra argument of type `rsize_t` that specifies the maximum length of the destination buffer.

The `strcpy_s()` function is similar to `strcpy()` when there are no constraint violations. The `strcpy_s()` function copies characters from a source string to a destination character array up to and including the terminating null character. The function returns zero upon success.

The `strcpy_s()` function only succeeds when the source string can be fully copied to the destination without overflowing the destination buffer. If either the source or destination pointers are NULL or if the maximum length of the destination buffer is equal to zero, greater than RSIZE_MAX, or less than or equal to the length of the source string, the destination string is set to the null string and the function returns a nonzero value.

The `strcat_s()` function appends the characters of the source string, up to and including the null character, to the end of the destination string. The initial character from the source string overwrites the null character at the end of the destination string.

The `strcat_s()` function returns zero on success. However, the destination string is set to the null string and a nonzero value is returned if either the source or destination pointers are NULL or if the maximum length of the destination buffer is equal to zero or greater than RSIZE_MAX. The `strcat_s()` function will also fail if the destination string is already full or if there is not enough room to fully append the source string.

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/268-BSI.html (Plakosh, Daniel)

The `strcpy_s()` and `strcat_s()` functions can still result in a buffer overflow if the maximum length of the destination buffer is incorrectly specified.

References

[ISO/IEC 99]	ISO/IEC. *ISO/IEC 9899 Second edition 1999-12-01 Programming languages — C*. International Organization for Standardization, 1999.
[ISO/IEC 04]	ISO/IEC. *ISO/IEC WDTR 24731 Specification for Secure C Library Functions*. International Organization for Standardization, 2004.

Pearson Education, Inc. Copyright

This material is excerpted from *Secure Coding in C and C++*, by Robert C. Seacord, copyright © 2006 by Pearson Education, Inc., published as a CERT® book in the SEI Series in Software Engineering. All rights reserved. It is reprinted with permission and may not be further reproduced or distributed without the prior written consent of Pearson Education, Inc.